Assignments (*Computer Security and Privacy*)

Assignment #1
Submission Deadline: February 7, 2018
Maximum Marks: 30

In this programming assignment you will implement the Hill cipher in C/Python/Java. In particular you will implement and submit three independent programs

- KeyGen
- Encrypt
- Decrypt

These program shall perform the following functions:

- KeyGen: This program will take, as input, a positive integer m. It will output a random key K from the keyspace of Hill Cipher, that is a random $m \times m$ matrix K such that K is invertible over $\mathbb{Z}_{26}$. The key should be copied to a file named **key.txt**.
- Encrypt: Inputs to this program are two files - **key.txt** and **msg.txt**. The file msg.txt will contain messages over alphabet "a-z" (all in small case). No special characters are allowed. This program will implement Hill cipher encryption over the msg (in **msg.txt**) using the key (in **key.txt**) and copy the resulting ciphertext into **ciphertext.txt** file.
- Decrypt: Inputs to this program are two files - **key.txt** and **ciphertext.txt**. This program will implement Hill cipher decryption over the ciphertext (in **ciphertext.txt**) using the key (in **key.txt**) and copy the resulting message into **output.txt** file.

Important Instructions!!

- The implementation of Hill cipher requires you to build subprograms such as "gcd, modular inverse computation, matrix multiplication, matrix inversion over $\mathbb{Z}_{26}$. You cannot use libraries for these tasks. You have to implement these subprograms yourself.
- Programs that implement Hill cipher only for a fixed value of m - such as $m = 2, 3$ will not be accepted.
- 20 marks, out of 30, are for correctness. The rest 10 will account for programming efficiency and proficiency.